INGV - Istituto Nazionale di Geofisica e Vulcanologia

DPC - Dipartimento della Protezione Civile

Convenzione INGV-DPC 2004 – 2006

Progetto S2 - Realizzazione di un modello dinamico sperimentale di valutazione della pericolosità sismica a scala nazionale

Project S2 - Development of a dynamical model for seismic hazard assessment at national scale

CrisisWeb Installation Manual

By UR3 – INGV Milano-Pavia
Francesco Martinelli & Carlo Meletti

(ver. 1.2.1)

24th August 2009

Indice

1 Premessa

Il presente manuale serve come riferimento per l'installazione dell'applicazione CrisisWeb e per le operazioni di gestione da parte dell'amministratore del sito.

2 Configurazione del server

L'applicazione è stata sviluppata con tecnologia Microsoft, utilizzando il framework .NET versione 3.5, ed utilizzando come web server/application server IIS versione 5.1, su sistema operativo Windows XP Profesional, versione 2002, service pack 3.

L'applicazione è stata rilasciata e testata su un server con le seguenti caratteristiche:

- S.O.: Windows Server Enterprise 6.0 con Service Pack 1
- IIS 7.0

Per la gestione degli utenti è stato attivato il sistema di appartenenze ASP.NET, con il provider predefinito AspNetSqlMembershipProvider, utilizzando come database aspnetdb nel computer SQL Server locale.

Di conseguenza è necessario che sul server sia installato ed attivato il servizio SQLEXPRESS.

3 Installazione dell'applicazione

L'applicazione viene rilasciata come file .ZIP da scompattare nella directory che verrà poi assegnata come percorso fisico del sito Web.
Assicurarsi che sia presente la cartella Images, anche se vuota.

Deve essere creata una specifica cartella per i dati degli utenti, che può trovarsi ovunque, purché sulla stessa macchina (ovvero anche un disco differente).
Tale cartella deve avere una sottocartella denominata "**super**".

I file **ASPNETDB.MDF** e **aspnetdb_log.ldf** sono quelli utilizzati dal provider delle appartenenze e possono essere spostati dalla cartella App_Data in qualsiasi altra del file system.
In particolare, tali file devono essere resi accessibili in lettura ed in scrittura all'utente che di sistema che li accede (*probabilmente il gruppo IIS_IUSRS potrebbe essere più appropriato*) .
Nell'ambiente di test al gruppo di sistema "User" è stato dato il controllo completo su questi due file.

La cartella "**Crisis2008IniFiles"** deve essere messa nella root del driver C.

Tramite IIS creare il sito Web per l'applicazione, indicando come percorso fisico quello dove è stato compattato il file .ZIP.

4 Configurazione dell'applicazione

L'applicazione utilizza come strumento di logging "`log4net`", configurabile nella sezione `<log4net>` del file Web.config. Per i dettagli della configurazione fare riferimento al sito http://logging.apache.org/log4net/

Modificare i seguenti elementi del file Web.config della root del sito:

- L'elemento **<log4net>** viene rilasciato configurato per utilizzare come "appender" il RollingFileAppender. Il nome del file di log è specificato all'interno dell'elemento <appender>, come attributo dell'elemento <file>. Altri elementi significativi di appender sono:
  - <maxSizeRollBackups> per indicare il numero di file di backup da mantenere prima di sovrascriverli;
  - <maximumFileSize> per indicare la dimenzione del file di log prima di iniziarne uno nuovo.
- Modificare l'attributo value dell'elemento <level> dell'elemento <root> dell'elemento <log4net> ad uno dei seguenti valori, a seconda del tipo di livello di logging (valori forniti in ordine di dettaglio crescente): ERROR, WARN, INFO. Si raccomanda di non utilizzare i valori DEBUG (troppo dettagliato) o FATAL (non utilizzato).
- Nell'elemento <appSettings> modificare l'attributo value dell'elemento con attributo key="RootDirectoryForUserData". Tale valore corrisponde al percorso completo della cartella per i dati degli utenti precedentemente creata.
- Nell'elemento <appSettings> modificare l'attributo value dell'elemento con attributo key="AdministratorEmailAddress". Tale valore corrisponde all'indirizzo di email che verrà fornito agli utenti nella pagina di Console.
- Nell'elemento <connectionString> modificare il seguente elemento:

```
<add name="LocalSqlServer"
  connectionString = "Data Source=.\SQLExpress;Integrated
Security=True;User
Instance=True;AttachDBFilename=C:\CrisisWeb\App_Data\ASPNETDB
.MDF"
  providerName="System.Data.SqlClient"/>
```

  in modo che la parte AttachDBFilename corrisponda al percorso dove è stato posizionato il file ASPNETDB.MDF.
- Nell'elemento <providers>,all'interno dell'elemento <membership>, modificare, se necessario, gli attributi del seguente elemento:

```
<add connectionStringName="LocalSqlServer"
  enablePasswordRetrieval="false"
  enablePasswordReset="true"
  requiresQuestionAndAnswer="true"
  applicationName="/CrisisWeb"
  requiresUniqueEmail="false"
  passwordFormat="Hashed"
  maxInvalidPasswordAttempts="5"
  minRequiredPasswordLength="3"
  minRequiredNonalphanumericCharacters="0"
  passwordAttemptWindow="10"
  passwordStrengthRegularExpression=""
  name="AspNetSqlMembershipProvider"
  type="System.Web.Security.SqlMembershipProvider,
System.Web, Version=2.0.0.0, Culture=neutral,
PublicKeyToken=b03f5f7f11d50a3a" />
```

  In particolare i seguenti attributi dovrebbero essere lasciati invariati:
  - connectionStringName
  - enablePasswordRetrieval
  - enablePasswordReset
  - requiresQuestionAndAnswer
  - applicationName
  - name
  - type

- Impostare l'elemento `<customErrors>` con l'attributo **`mode`** a "`RemoteOnly`" oppure "`Off`", ed eventualmente gli elementi `<error>` delle pagine per errori specifici.
- Modificare l'attributo `maxRequestLength` dell'elemento `<httpRuntime>` per consentire di fare l'upload di file fino alla dimensione indicata nell'attributo. Il numero fornito si intende relativo a KB. Non è possibile fornire un valore corrispondente ad "illimitato".
- Modificare l'elemento `<smtp>` dell'elemento `<mailSettings>` dell'elemento `<system.net>` in modo da fornire un account valido da cui poter inviare email per conto dell'applicazione (reset di password). Ad es.:

```
  <smtp from="utenteApparente@ingv.it">
    <network host="1.2.3.4" password="pwdUtente"
userName="utente" />
  </smtp>
```

  Si raccomanda di mantenere uguali i due valori in grassetto (utenteApparente e utente).

5 Test dell'installazione

L'applicazione viene rilasciata con un utente con ruolo **super**, il cui UserName è "Super", e la cui password è "super".

Accedere al sito dell'applicazione.
Il browser dovrebbe indirizzare sulla pagina Logon.aspx
In caso contrario verificare la correttezza dell'installazione, anche tentando di accedere direttamente alla pagina Logon.aspx

Accedere con UserName Super, e password super.
Nel caso venga visualizzata la pagina Console dell'amministratore il database del provider delle appartenenze è stato correttamente installato.
In caso contrario, provare ad assegnare al gruppo di utenti "User" il controllo completo sui file del database (**ASPNETDB.MDF** e **aspnetdb_log.ldf**); far ripartire il server (per sicurezza) e ripetere il tentativo di accesso.
In caso di successo modificare opportunamente i privilegi sui file, riavviare il server e testare nuovamente fino ad avere un assegnamento di privilegi soddisfacente dal punto di vista della sicurezza (se richiesto).
In caso di fallimento è possibile il problema sia di errore nell'impostazione dell'elemento `<connectionString>`.

6 Creazione e Gestione degli utenti

[Da fare dopo l'aggiornamento delle pagine di amministrazione]

7 Note

Attualmente il database delle appartenenze non offre molte garanzie di sicurezza; inoltre le informazioni presenti non sono crittografate.
Peraltro tale database contiene le seguenti informazioni:

- account utente
- password utente
- domanda privata
- risposta privata

- indirizzo di email
- altri dati relativi agli accessi effettuati.

Un’eventuale intrusione e diffusione di tali dati permetterebbe all’intruso di conoscere gli indirizzi di email degli utenti. Inoltre permetterebbe di accedere alle aree private degli utenti permettendo via web di:

- cancellare eventuali file presenti
- fare upload sul server di file dell’intruso

Non sarebbe però comunque possibile via web mandare in esecuzione tali file, in quanto non sono direttamente accessibili.
Si ritiene che le informazioni di nome account, password, domanda e risposta segreta e dati sugli accessi effettuati non siano di alcun valore.

Per quanto riguarda gli indirizzi di email si ritiene siano un dato non particolarmente sensibile.

Le due operazioni sopra descritte sulle aree private è poco probabile vengano attuate con strumenti automatici, e quindi sarebbe necessaria la volontà specifica di accedere il server per danneggiarne i dati: cosa poco probabile, ma che comunque può essere facilmente mitigata da backup fatti sulla cartella dei dati utente.

Lo sforzo richiesto per aumentare la sicurezza del database non sembra pertanto attualmente giustificato.